

## UNITED STATES DISTRICT COURT

for the  
Western District of New York

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
Associated file of Cyberline Report 183378675

Case No. 24-MJ-521-MJP

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
Associated file of Cyberline Report 183378675, more fully described in Attachment A, which is incorporated by reference as if fully set forth herein.

located in the Western District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is incorporated by reference as if fully set forth herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2252A(a)(5)(B)	Possession of Child Pornography
18 USC 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography

The application is based on these facts:  
See attached affidavit by Federal Bureau of Investigation (FBI) Task Force Officer (TFO) Christopher Toscano.

- ☒ Continued on the attached sheet.  
☒ Delayed notice of 90 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Christopher Toscano, FBI TFO  
Printed name and title

Sworn to before me and signed in my presence.

Date: February 27, 2024

City and state: Rochester, New York

  
Judge's signature

Hon. Mark W. Pedersen, U.S. Magistrate Judge  
Printed name and title

**ATTACHMENT A**

**ITEMS TO BE SEARCHED**

Associated file of **Cybertipline Report 183378675**, that was forwarded to the National Center for Missing and Exploited Children (NCMEC) by Facebook (Meta Platforms Inc.); which is currently in the custody of the Federal Bureau of Investigation, located at 1200 Scottsville Road Building C. Suite 300, Rochester, New York, 14624.

**ATTACHMENT B**  
**ITEMS TO BE SEIZED AND SEARCHED**

Any and all files containing a visual depiction of a minor, to include images and videos of children engaged in sexually explicit conduct as described in 18 U.S.C. § 2256, nude pictures, and modeling. Additionally, any communication, information, picture, video or documentation that identifies the user of the account or that indicates a sexual interest in children.

**AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT**

I, CHRISTOPHER TOSCANO, being duly sworn, depose and state:

1. I am a Deputy with the Monroe County Sheriff's Office and have been assigned as a Task Force Officer (TFO) with the FBI's Child Exploitation and Human Trafficking Task Force since 2017. As a TFO, I am responsible for investigating the production, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), and 2252A(a)(5)(B). I have been involved in hundreds of federal child pornography investigations and have seen thousands of images of child pornography as defined by 18 U.S.C. § 2256(8).

2. This affidavit is made in support of an application for a warrant to search the associated file of **CyberTipline Report 183378675** that was forwarded to the National Center for Missing and Exploited Children (NCMEC) by Facebook (Meta Platforms, Inc.) ("TARGET REPORT").

3. The TARGET REPORT is to be searched for evidence of violations of Title 18 U.S.C. § 2252A(a)(2)(A) (distribution/receipt of child pornography) and Title 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) (the "TARGET OFFENSES").

4. The information contained in this affidavit is based upon my personal knowledge and observations, my training and experience, conversations with other law enforcement officers, and my review of documents and records related to this case to include the TARGET REPORT.

5. Since this affidavit is being submitted for the limited purpose of establishing probable cause to secure a search warrant, I have not included every fact known to me

concerning this investigation. Rather, I have set forth facts that I believe are relevant to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of the TARGET OFFENSES are located in the TARGET REPORT.

#### **NCMEC CYBERTIPLINE**

6. The National Center for Missing and Exploited Children (NCMEC) is a nonprofit organization that operates a “CyberTipline” through which internet and electronic service providers (ESP’s) are required to report the presence of child pornography on their platforms. The duties of ESPs and NCMEC to report child exploitation and child pornography are set forth in 18 U.S.C. § 2258A.

7. If NCMEC receives a child exploitation Cybertip, it utilizes information provided by the ESP to determine the general geographic area (such as the state) where the offender is located. NCMEC then forwards the tip to law enforcement for further investigation on the information provided in the Cybertipline report.

#### **FACEBOOK**

8. Facebook is a social networking site that is owned and operated by Meta Platforms Inc. Facebook allows users to sign-up and create a free profile to connect and interact with other individuals. One way users interact with one another is through the use of Facebook Messenger. Facebook Messenger allows users to send messages, photographs, and videos, thus in and affecting interstate and foreign commerce via the internet.

**PROBABLE CAUSE**

9. On December 31, 2023, Facebook sent **Cybertipline Report 183378675** to NCMEC and listed the Incident Type<sup>1</sup> as “Child Pornography” (possession, manufacture, and distribution).” The report was processed by NCMEC on December 31, 2023, and provided to law enforcement.

10. The report for **183378675** provided the following information regarding the Facebook user being reported:

Name: North Greece

Mobile Phone: +15854834865 (Verified)

ESP User ID: 61553191400565 (hereinafter “TARGET USER”)

Profile URL: <https://www.facebook.com/profile.php?id=61553191400565>

11. The report for **183378675** stated that the TARGET USER uploaded one file on December 28, 2023, at 17:26:23 UTC from IP address 68.172.160.213. Facebook further provided messages captured around the time of the uploaded file.

12. The following messages were provided by Facebook.

- a. TARGET USER – “So good”
- b. ESP User ID 61552154855677 – “oh yea so good you’re nice they are doing good young girls”
- c. TARGET USER – “Eating out little vagina is good”

---

<sup>1</sup> NCMEC Incident Type is based on a “Hash Match” of one or more uploaded files or NCMEC’s review of the report. “Hash matching” is a technological process through which an ESP can match an image or video to identical images or videos previously confirmed to depict child pornography as defined by 18 U.S.C. § 2256(8). NCMEC may not have viewed all uploaded files submitted by the reporting ESP.

13. In the Cybertipline Report, Facebook stated that they did not view the entire contents of the uploaded file but categorized the image as "A2." According to the categorization category, A2 is designated as "Prepubescent Minor" with "Lascivious Exhibition." A further definition provided is as follows, "Any imagery depicting the lascivious exhibition of the anus, genitals, or pubic area of any person, where a minor is engaging in the lascivious exhibition or being used in connection with sexually explicit conduct, which may include but is not limited to imagery where the focal point is on the child's anus, genitals, or pubic area and where the depiction is intended or designed to elicit a sexual response in the viewer."

14. To your affiant's knowledge, the uploaded file provided with the Cybertipline report has not been reviewed by members of law enforcement.

#### **TRAINING AND EXPERIENCE**

15. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

- a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

- b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals who have a sexual interest in children or images of children frequently maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.
- e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.
- f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer-to-Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child



pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

- g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

16. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

- a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.
- b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.
- c. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence.
- d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a

computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

- e. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.
- f. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.
- g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.
- h. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

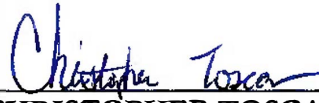
1. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the TARGET REPORT notwithstanding the passage of time.
- j. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.
- k. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.
- l. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.
- m. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

### **CONCLUSION**


17. Based upon the forgoing, I respectfully submit that there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of the TARGET OFFENSES, as specifically described in Attachment B to this application, are currently contained in the TARGET REPORT as further described in Attachments A1. I therefore

respectfully request that a search warrant be issued authorizing a search of the TARGET REPORT for the item described above and in Attachment B and authorizing the seizure and examination of any such items found therein.

18. Due to the ongoing nature of this investigation, and the possibility of seriously jeopardizing the effectiveness of the investigation if information were made public, I request that the search and seizure warrant, and this application be sealed until further order of the Court.

  
CHRISTOPHER TOSCANO  
Task Force Officer  
Federal Bureau of Investigation

Affidavit submitted electronically by email in .pdf format. Oath administered, and contents and signature attested to me as true and accurate telephonically pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on February 27, 2024.

  
HON. MARK W. PEDERSEN  
United States Magistrate Judge